PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-306092
(43)Date of publication of application : 05.11.1999

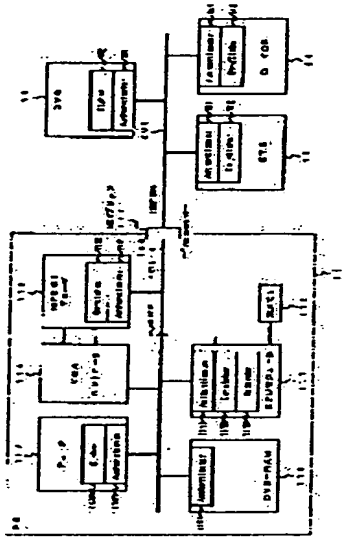
(51)Int.CI. G06F 12/16
G06F 12/14

(21)Application number : 10-108116
(22)Date of filing : 17.04.1998

(71)Applicant : TOSHIBA CORP
(72)Inventor : ISHIBASHI YASUHIRO
SOGABE HIDEKI

(54) DATA PROCESSOR AND COPY PROTECT SYSTEM APPLIED TO THE PROCESSOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide protection of digital contents flowing on a bus of a computer system and limit of the digital contents for each function module.
SOLUTION: With regard to a CPU module 111, a tuner 113 for a satellite or digital TV, an MPEG 2 decoder 115, and a DVD-RAM drive 116, an interface part with a PCI bus 100 is provided with authentication processing parts (authenticators) 1111, 1131, 1151 and 1161 for performing equipment authentication, key exchange and the like. In this way, providing each function module with a authentication function for enciphering processing, it becomes possible to efficiently realize protection of digital contents flowing on the PCI bus 200 connecting between the function modules, and limit of the digital contents for each function module.



LEGAL STATUS

[Date of request for examination] 24.03.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] In the data processor which has an interface with the external bus which can connect the external instrument which has an authentication function for enciphering, delivering and receiving the data for a copy protection An internal bus and two or more functional modules which are combined with this internal bus, respectively, and transmit or receive the data for a copy protection via [aforementioned] an internal bus, Between the functional modules of the partner point or the aforementioned external instruments which are prepared for every aforementioned functional module, and deliver and receive the data for [aforementioned] a copy protection The data processor characterized by providing an authentication means to perform authentication processing for enciphering, delivering and receiving the data for [aforementioned] a copy protection, and performing authentication processing for every functional module in the aforementioned data processor.
[Claim 2] The data processor according to claim 1 characterized by to prepare an encryption means encipher the data for [aforementioned] a copy protection in the functional module of the transmitting side which transmits the data for [aforementioned] a copy protection through the aforementioned internal bus, and to prepare the decryption means for decrypting the data by which encryption was carried out [aforementioned] and canceling the encryption in the functional module of the receiving side which minds the aforementioned bus, and receives and processes the data for [aforementioned] a copy protection.
[Claim 3] The data processor according to claim 2 characterized by transmitting encryption data on the aforementioned external bus and an internal bus, and using the same authentication and an encryption protocol on the both sides between [aforementioned] functional modules and between the aforementioned external instrument and the aforementioned functional module when an external bus interface means to connect between the aforementioned external bus and the aforementioned internal buses transparent is provided further and the data for a copy protection are delivered and received between the aforementioned external instrument and each aforementioned functional module.
[Claim 4] the functional module treating the data for [aforementioned] a copy protection -- being alike -- CPU module, the decoder which decodes the coded data by which digital compression coding was carried out, and the data processor according to claim 1 characterized by containing at least one of storage devices
[Claim 5] The data once which can be copied, and the data which cannot be copied are in the modality of data for [aforementioned] a copy protection. to each aforementioned functional module The identification information for specifying the modality of data which can be treated by the functional module is assigned. the aforementioned authentication means It distinguishes whether it is a functional module with the functional module of the receiving side able to treat the data for sending based on the identification information corresponding to the functional module of a receiving side. When it is the functional module which can treat the data for sending, The data processor according to claim 1 characterized by performing key exchange for making the functional module of a receiving side generate an encryption cancel key required in order to decrypt encryption data between the functional modules of a receiving side.

[Claim 6] When transmitting the stream which consists of two or more sorts of data with which an encryption cancel key required in order to decrypt the enciphered data is changed for every modality of data for sending, and a modality is different, The data processor according to claim 1 characterized by generating the encryption cancel key of the number corresponding to the number of modalities of the data which can process the functional module of a receiving side by the aforementioned authentication processing in the modality of data which constitute the aforementioned stream on the functional module of the aforementioned receiving side.
[Claim 7] It is the data processor according to claim 6 which the data class information which shows the modality of data is embedded at the aforementioned stream, and is characterized by the functional module of the aforementioned receiving side changing dynamically the encryption cancel key used based on the aforementioned data class information.
[Claim 8] It is the data processor according to claim 1 characterized by for the aforementioned data processors being CPU module, the decoder which decodes the coded data by which digital compression coding was carried out, and a personal computer which has a storage device as the aforementioned functional module, and for this personal computer having a PCI bus as the aforementioned internal bus, and having an IEEE1394 serial bus as the aforementioned external bus.
[Claim 9] In the data processor which has a bus and two or more functional modules combined with this bus, respectively Each functional module which treats digital contest ****** for a copy protection in two or more aforementioned functional modules Between the functional modules of the partner point which delivers and receives digital contest ****** through the aforementioned bus The contents [an authentication means to perform authentication processing for enciphering, delivering and receiving the aforementioned digital contest ****** is provided, and / the modality of digital contents for / aforementioned / a copy protection] once which can be copied, There is a contents [that it cannot copy] and the modality of contents which can be treated by the functional module is specified for every aforementioned functional module. the aforementioned authentication means The data processor characterized by distinguishing whether it is a functional module with the functional module able to treat the contents for sending for every functional module of a receiving side.
[Claim 10] An internal bus and two or more functional modules which are combined with this internal bus, respectively, and transmit or receive the data for a copy protection via [aforementioned] an internal bus, In the copy protection technique applied to the data processor possessing an external bus interface means to connect between the external buses and the aforementioned internal buses which can connect the external instrument which has the data encryption / decryption function for a copy protection Between the aforementioned external bus and the aforementioned system buses is connected transparent by the aforementioned external bus interface means. When delivering and receiving the data for a copy protection between [aforementioned / two or more] functional modules or between the aforementioned functional module and an external instrument, When authentication processing for checking the justification of a mutual functional module between [for a communication] devices is performed and the justification of a mutual device is checked by this authentication processing, Encipher transmit data in the device of a transmitting side, and it transmits to the device of the partner point. The copy protection technique characterized by carrying out the copy protection of the both sides of the data which decrypt the encryption data in the device of a receiving side, and flow on the aforementioned system bus, and the data which flow to the aforementioned external bus.
[Claim 11] It is the copy protection technique of the digital contents applied to the system which consists of a bus and two or more devices connected to this bus. When the stream which consists of two or more sorts of digital contentss from which a modality is different is enciphered and it transmits to the device of a receiving side, the device of a transmitting side Only the number of modalities of the contents which precedes the sending and it can treat for every device of a receiving side by performing authentication processing The encryption cancel key corresponding to the number of modalities of the data which can process the device of a receiving side in the modality of digital contents which constitutes the aforementioned stream is notified to the device

of each receiving side. The device of a receiving side is the copy protection technique characterized by changing the encryption cancel key to use according to the modality of digital contents which received.
[Claim 12] It is the copy protection technique according to claim 11 which the class information which shows the modality of digital contents is embedded at the aforementioned stream, and is characterized by the device of a receiving side changing dynamically the encryption cancel key used for decryption processing based on the aforementioned data class information.
[Claim 13] In the data processor which transmits data to a receiving set side so that the unjust copy of the digital contents passed on an internal bus may be prevented An authentication means to attest whether processing of the data for a copy protection is permitted between the aforementioned receiving sets, A judgment means by which the data for a copy protection with which processing is permitted to the aforementioned receiving set distinguish what kind of digital contents it is when attested by the aforementioned authentication means, A key transmitting means to transmit the encryption cancel key corresponding to the modality of digital contents by which processing is permitted to the aforementioned receiving set to the aforementioned receiving set based on the judgment result of this judgment means, respectively, The data processor to which the aforementioned receiving set is characterized by providing a transmitting means to transmit the digital contents which can cancel an encryption using the aforementioned encryption cancel key.
[Claim 14] So that the unjust copy of the digital contents passed on the internal bus of a computer system may be prevented It is the copy protection technique of transmitting data to a receiving set side proper. It attests whether processing of the data for a copy protection is permitted between the aforementioned receiving sets. When attested, the data for a copy protection with which processing is permitted to the aforementioned receiving set Distinguish what kind of digital contents it is, and it is based on this judgment result. Only the encryption cancel key corresponding to the modality of digital contents by which processing is permitted to the aforementioned receiving set is transmitted to the aforementioned receiving set, respectively. The copy protection technique that the aforementioned receiving set is characterized by transmitting the digital contents which can cancel an encryption using this encryption cancel key.
[Claim 15] In the data processor which carries out reception of the data transmitted from the sending set side so that the illegal copy of the digital contents passed on an internal bus might be prevented An authentication means to attest whether processing of the data for a copy protection is permitted between the aforementioned sending sets, A modality information transmitting means to transmit the information which shows the modality of digital contents for [by which processing is permitted to this data processor] a copy protection when attested by the aforementioned authentication means to the aforementioned sending set, The encryption cancel key respectively corresponding to the modality of digital contents for [by which processing is permitted to the aforementioned data processor based on this modality information] a copy protection, The data processor characterized by providing a decryption means to receive the digital contents of which the aforementioned data processor can cancel an encryption using this encryption cancel key from the aforementioned sending set, and to decrypt the aforementioned digital contents.
[Claim 16] So that the unjust copy of the digital contents passed on the internal bus of a computer system may be prevented It is the copy protection technique which carries out reception of the data proper from a sending set side. It attests whether processing of the data for a copy protection is permitted between the aforementioned sending sets. When attested, the information which shows the modality of digital contents for [to which the reception of data is permitted] a copy protection is transmitted to the aforementioned sending set. Based on this modality information, the encryption cancel key corresponding to the modality of digital contents to which the aforementioned reception is permitted is received from the aforementioned sending set, respectively. The copy protection technique characterized by for a receiving set receiving the digital contents which can cancel an encryption from the aforementioned sending set, and decrypting the aforementioned digital contents using the aforementioned encryption cancel key using this encryption cancel key.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[The technical field to which invention belongs] this invention relates to the copy protection technique applied to the data processor which has an interface with external buses, such as an IEEE1394 serial bus, especially, and this equipment about the copy protection technique of the digital contents used with a data processor and these equipments, such as a personal computer.

[0002]

[Description of the Prior Art] In recent years, in connection with development of computer technique, the electronic equipment of multimedia correspondence, such as a digital video player, a set top box, TV, and a personal computer, is developed variously.

[0003] This kind of electronic equipment can reproduce digital contentss, such as TV program by the movie and digital satellite broadcasting which were accumulated at DVD (Digital VersatileDisk).

[0004] A digital contents is sent to each home through a record medium and a transmission medium, after encoding generally using a dynamic-image bandwidth compression method called MPEG 2. Coding by MPEG 2 is based on the idea of a viewpoint to adjustable rate coding which secures quality of image and the both sides of a chart lasting time to capacity. In the amount of data of adjustable rate coded data, depending on the quality of image of the original picture image, the amount of data increases the more intense scene of a motion. Therefore, a digital contents can offer the high-definition picture which does not have an original picture and inferiority in each home.

[0005] The present condition is that effective technique is not built from viewpoints, such as copyright protection of such a digital contents, in recent years although cried for the need for the copy protection technique for preventing the illegal copy.

[0006] Then, in CPTWG (Copy Protection TechnicalWorking Group), decision work of the specification (IEEE1394 copy-protection technique is called hereafter) of the new copy protection method towards the IEEE1394 serial bus which is the bus interface of the suitable next generation for a transmission of multimedia data is done.

[0007] It is the bus interface of the next generation which connects a digital video player, a set top box, TV, a personal computer, etc., and an IEEE1394 serial bus is a ****** clo eggplant as transfer mode. As isochronous as a sub action Two kinds of sub actions are supported. The former is called Asynchronous Transfer Mode and used at the time of the general data transfer as which real time nature is not required. The latter is the synchronous transfer mode which guaranteed the transfer band, and the real-time transfer of the digital contents represented by a video data and audio data is possible for it.

[0008] IEEE1394 copy-protection technique enciphers the digital contents delivered through an IEEE1394 serial bus among devices, such as a digital video player, a set top box, TV, and a personal computer, and enables it to prevent the illegal copy by using the encryption protocol which a public-key-encryption-ized method, a common key cipher system, etc. are good, and was known.

[0009]

[Problem(s) to be Solved by the Invention] However, since a personal computer is a system open from the first, it cannot expect sufficient protection to an illegal copy only by enciphering the data which flow on an IEEE1394 serial bus. Hereafter, this is explained concretely.

[0010] Drawing 15 is an example of a configuration at the time of applying IEEE1394 copy-protection technique to a personal computer as it was. In drawing 15 , a mode that a personal computer (PC) 1, the set top box (STB) 2, and three devices of a digital camcorder (DVC) 3 are connected through the IEEE1394 serial bus 10 is shown.

[0011] These personal computers (PC) 1, the set top box (STB) 2, and the digital camcorder (DVC) 3 have the encryption section (Cipher), the decryption section (De-Cipher), or encryption/decryption section (De-/Cipher) with both function of encryption and a decryption among the interface section with the IEEE1394 serial bus 10, respectively.

[0012] namely, -- IEEE -- 1394 -- serial -- a bus -- ten -- minding -- others -- a device -- digital -- a contents -- sending -- carrying out -- a digital camcorder (DVC) -- three -- ******** -- encryption -- the section (Cipher) -- preparing -- having -- IEEE -- 1394 -- serial -- a bus -- ten -- minding -- others -- a device -- between -- digital -- a contents -- transmission and reception -- carrying out -- a personal computer -- (-- PC --) -- one -- and -- a set top box (STB

[0013] The digital contents which needs a copy protection is outputted on the IEEE1394 serial bus 10, after enciphering by the device of the transmitting side, the encryption data is decrypted by the device of a receiving side, and encryption is canceled. Thus, by enciphering the data which flow on the IEEE1394 serial bus 10, even if the data which flow on the IEEE1394 serial bus 10 are copied unjustly, it can prevent that it will be reproduced normally.

[0014] In a personal computer (PC) 1, encryption/decryption section (De-/Cipher) is prepared like illustration in 1394 bridges 6 which connect between system buses, such as PCI bus 20, and the IEEE1394 serial buses 10 with both directions. Thereby, since encryption data do not flow, but it usually passes on PCI bus 20 and only plaintext data flow, open bus architecture is maintainable.

[0015] After the encryption data transmitted to a personal computer (PC) 1 through the IEEE1394 serial bus 10 from the digital camcorder (DVC) 3 or the set top box (STB) 2 are decrypted by 1394 bridges 6 at a plaintext, they are sent to CPU4 and the MPEG decoder 5 on PCI bus 20. When transmitting a digital picture contents to a set top box (STB) 2 from CPU4 or the MPEG decoder 5, after the plaintext on PCI bus 20 is similarly enciphered by 1394 bridges 6, it delivers on the IEEE1394 serial bus 10.

[0016] Thus, if encryption/decryption function is prepared in 1394 bridges 6, although the open architecture of PCI bus 20 is maintainable as it is, the data (Plain Contents) with which encryption was solved by PCI bus 20 will flow, and a copy will become possible easily.

[0017] Moreover, in the personal computer of the drawing 15 which prepared encryption/decryption function in 1394 bridges 6, it becomes difficult to perform control of restricting the modality (only 1 time a copy good, copy improper, a copy free-lancer) of contents which constitutes a personal computer and which the functional module can treat for every functional module. For example, it is necessary for storage devices, such as DVD-RAM and HDD, to be able to treat only the contents once which can be copied, and a copy free-lancer's contents, and for things to be made not to be made to enabling it to treat the contents (only 1 time a copy good, copy improper, a copy free-lancer) of all modalities about MPEG 2 decoder. However, it is Plain to PCI bus 20. If Contents flows, it is difficult to restrict the contents which it can treat for every functional module in practice. It is because such a limit of a contents is usually performed by authentication processing between devices. That is, when encryption/decryption function is prepared in 1394 bridges 6, a personal computer is also treated as one device on an IEEE1394 serial bus. For this reason, although it is possible to restrict the modality of contents which can treat the personal computer by authentication processing between a personal computer and other devices on an IEEE1394 serial bus, the modality of contents cannot be restricted per each module in a personal computer.

[0018] Moreover, in DVD video etc., the digital contents is realized in many cases as a stream containing two or more contentss from which a modality is different. In this case, although the modality of contents for regeneration will change dynamically, in having done authentication again, whenever the modality of contents changed, there is also a problem that it becomes impossible to process a contents on real time.

[0019] this invention is made in view of the above-mentioned actual condition, and it enables it to realize protection of the digital contents which flows on the bus in data processors, such as a personal computer, and a limit of the digital contents in the functional-module unit which constitutes a data processor, and aims at offering the copy protection technique applied to the data processor which can perform the copy protection of a digital contents efficiently, and this equipment.

[0020]

[Means for Solving the Problem] In the data processor which has an interface with the external bus which can connect the external instrument which has an authentication function for this invention

enciphering, delivering and receiving the data for a copy protection in order to solve an above-mentioned technical probrem An internal bus and two or more functional modules which are combined with this internal bus, respectively, and transmit or receive the data for a copy protection via [aforementioned] an internal bus, Between the functional modules of the partner point or the aforementioned external instruments which are prepared for every aforementioned functional module, and deliver and receive the data for [aforementioned] a copy protection An authentication means to perform authentication processing for enciphering, delivering and receiving the data for [aforementioned] a copy protection is provided, and it is characterized by performing authentication processing for every functional module in the aforementioned data processor.

[0021] In this data processor, the authentication means is prepared in the interface section of two or more functional modules of each treating the data for [, such as a digital contents,] a copy protection, and authentication processing is individually performed between functional modules or between a functional module and an external instrument. Therefore, on the internal bus to which these functional modules were connected, the key and digital contents for encryption cancel come to be transmitted while it had been enciphered by them, and they can prevent the illegal copy of a digital contents. Moreover, since authentication processing is performed for every functional module, it is enabled to restrict efficiently the modality (only 1 time a copy good, copy improper, a copy free-lancer) of digital contents which can be treated by it per functional module.

[0022] Moreover, it is enabled to enable it to use the same authentication and an encryption protocol on the both sides between [aforementioned] functional modules and between the aforementioned external instrument and the aforementioned functional module by providing further an external bus interface means to connect between the external bus which can connect the external instrument which has the data encryption / decryption function for a copy protection, and the buses in the aforementioned data processor transparent. That is, it is enabled to treat similarly, without distinguishing the functional module and external instrument in a data processor, if it sees from each functional module or application program in a data processor.

[0023] The data once which can be copied, and the data which cannot be copied are in the modality of data for [aforementioned] a copy protection. moreover, to each aforementioned functional module The identification information for specifying the modality of data which can process the functional module is assigned. the aforementioned authentication means It is desirable to distinguish whether it is a functional module with the functional module of the aforementioned sending place able to treat the data for [aforementioned] sending based on the modality of data for sending and the identification information (system ID) of the functional module of a sending place.

[0024] Thus, by using a system ID, it is enabled to manage easily the modality of digital contents which can be treated per functional module. Moreover, as for an encryption cancel key required in order to decrypt the enciphered data, it is desirable to change for every (for a copy good and a copy to be impossible once) modality of data for sending. When this notifies only the key according to the contents which can treat it to each functional module for example, at the time of authentication processing, even if it is the case where the broadcasting transfer of the encryption contents is carried out at two or more functional modules, it is enabled to restrict so that only the functional module which can treat the contents can perform the decode.

[0025] Moreover, when transmitting the stream which consists of two or more sorts of data with which a modality is different, as for the aforementioned authentication means, it is desirable to notify the encryption cancel key corresponding to the number of modalities of the data which can process the functional module of a sending place in the modality of data with which only the number of modalities of the contents which the functional module of a sending place can treat performs authentication processing, and constitutes the aforementioned stream to the functional module of the aforementioned sending place. Thus, even if the modality of contents is dynamically changed by passing the encryption cancel key for every modality of contents beforehand to the functional module of a receiving side, it is enabled to cancel encryption on real time. In this case, the data class information which shows the modality of data is embedded at the stream, and a

decryption means should just change dynamically the encryption cancel key used for decryption processing based on the aforementioned data class information.
[0026] Moreover, this invention is set to the data processor which transmits data to a receiving set side so that the unjust copy of the digital contents passed on an internal bus may be prevented. An authentication means to attest whether processing of the data for a copy protection is permitted between the aforementioned receiving sets, A judgment means by which the data for a copy protection with which processing is permitted to the aforementioned receiving set distinguish what kind of digital contents it is when attested by the aforementioned authentication means, A key transmitting means to transmit the encryption cancel key corresponding to the modality of digital contents by which processing is permitted to the aforementioned receiving set to the aforementioned receiving set based on the judgment result of this judgment means, respectively, The aforementioned receiving set is characterized by providing a transmitting means to transmit the digital contents which can cancel an encryption using the aforementioned encryption cancel key.
[0027] In this data processor, it is attested whether processing of the data for a copy protection is permitted between the aforementioned receiving sets. When attested, the data for a copy protection with which processing is permitted to the aforementioned receiving set Only the encryption cancel key corresponding to the modality of digital contents by which it is distinguished what kind of digital contents it is, and processing is permitted to the aforementioned receiving set based on this judgment result is transmitted to the aforementioned receiving set, respectively. And the digital contents of which the aforementioned receiving set can cancel an encryption using this encryption cancel key is transmitted to a receiving set.
[0028] Moreover, this invention is set to the data processor which carries out reception of the data transmitted from the sending set side so that the illegal copy of the digital contents passed on an internal bus might be prevented. An authentication means to attest whether processing of the data for a copy protection is permitted between the aforementioned sending sets, A modality information transmitting means to transmit the information which shows the modality of digital contents for [by which processing is permitted to this data processor] a copy protection when attested by the aforementioned authentication means to the aforementioned sending set, The encryption cancel key respectively corresponding to the modality of digital contents for [by which processing is permitted to the aforementioned data processor based on this modality information] a copy protection, The digital contents of which the aforementioned data processor can cancel an encryption using this encryption cancel key is received from the aforementioned sending set, and it is characterized by providing a decryption means to decrypt the aforementioned digital contents.
[0029] In this data processor, it is attested whether processing of the data for a copy protection is permitted between the aforementioned sending sets, and when attested, the information which shows the modality of digital contents for [to which the reception of data is permitted] a copy protection is transmitted to the aforementioned sending set. And based on a modality information, the encryption cancel key corresponding to the modality of digital contents to which the aforementioned reception is permitted is received from the aforementioned sending set, respectively, and the digital contents of which a receiving set can subsequently cancel an encryption using this encryption cancel key is received from the aforementioned sending set. And the aforementioned digital contents is decrypted using the aforementioned encryption cancel key.
[0030]
[Embodiments of the Invention] Hereafter, the operation gestalt of this invention is explained with reference to a drawing. The system configuration of the personal computer (PC is called hereafter) concerning the 1 operation gestalt of this invention is shown in drawing 1 . this -- PC -- 11 -- IEEE -- 1394 -- serial -- a bus -- 200 -- minding -- the exterior -- consumer -- electronic equipment -- for example, -- illustration -- like -- a set top box (STB) -- 12 -- a digital camcorder -- or -- DV -- a camcorder (DVC) -- 13 -- and -- digital -- a video cassette recorder (D-VCR) -- 14 -- a communication -- possible -- constituting -- having -- **** .
[0031] The set top box (STB) 12, the digital camcorder (DVC) 13, and the digital video cassette recorder (D-VCR) 14 have the authentication processing section (Authenticator) 121,131,141

which performs device authentication, key exchange, etc. among the interface section with the IEEE1394 serial bus 200, in order to support IEEE1394 copy-protection technique, respectively. About the set top box (STB) 12 and the digital video cassette recorder (D-VCR) 14 which transmit and receive a digital contents, encryption/decryption section (De-/Cipher) 122,142 with both function of encryption and a decryption is formed. Moreover, only the encryption section (Cipher) 132 is formed about the digital camcorder (DVC) 13 which performs only sending of a digital contents.

[0032] The IEEE1394 serial bus 200 top is transmitted to the digital contents delivered and received between PC11, the set top box (STB) 12, the digital camcorder (DVC) 13, and the digital video cassette recorder (D-VCR) 14 in the status that it was enciphered.

[0033] PC11 consists of PCI bus 100 and two or more functional modules connected to this like illustration. In these functional modules, the authentication processing sections (Authenticator) 1111, 1131, 1151, and 1161 which perform device authentication, key exchange, etc. among the interface section with PCI bus 100 are formed about the tuner 113 for the functional module 111 treating digital contest ******, i.e., CPU module, a satellite, or digital TV, the MPEG 2 decoder 115, and the DVD-RAM drive 116. The function of each [these] authentication processing sections (Authenticator) 1111, 1131, 1151, and 1161 performs authentication required [it is the same as that of it of the set top box (STB) 12 which is 1394 devices, the digital camcorder (DVC) 13, and the digital video cassette recorder (D-VCR) 14 fundamentally, and] in order to encipher, deliver and receive a digital contents, and key exchange.

[0034] Moreover, the decryption section (De-cipher) which performs decryption processing for canceling encryption of the enciphered contents (encrypted contents) further, or the encryption section (Cipher) is prepared in the interface section of these CPUs module 111, the tuner 113, and the MPEG 2 decoder 115. It is decided by the function of each functional module whether it has the decryption section with the encryption section or it has the both. Here, the case where the encryption section (Cipher) 1132 is formed about a tuner 113, and the decryption sections (De-cipher) 1112 and 1152 are formed about the CPU module 111 and the MPEG 2 decoder 115 is illustrated.

[0035] The CPU module 111 consists of a microprocessor, a memory controller, PCI bus bridge, etc., and the authentication section 1111 and the encryption cancel section 1112 can be incorporated as for example, a part of PCI bus bridge. Moreover, software may realize the authentication section 1111 in the CPU module 111, the encryption cancel section 1112, and MPEG 2 decoder section 1113.

[0036] The DVD-RAM drive 116 is formed as auxiliary memory of PC11, and is connected to PCI bus 100 through IDE interface or ATAPI interface. The DVD-RAM drive 116 has only the authentication processing section 1161, and is not prepared about the decryption section (De-cipher) and the encryption section (Cipher). It is for recording on DVD-RAM116 with the status that the enciphered digital contents was enciphered.

[0037] 1394 bridges 117 which connect between PCI bus 100 and the IEEE1394 serial bus 200 in both directions are further established in PC11. No authentication processing sections, encryption sections, and decryption sections are prepared in 1394 bridges 117, but it passes through the enciphered digital contents IEEE1394 serial bus 200 from PCI bus 100 with the status that it was enciphered, and it is transmitted to PCI bus 100 from the IEEE1394 serial bus 200. Thus, 1394 bridges 117 connect between the functional module in PC11, and 1394 devices transparent.

[0038] Here, the procedure in the case of carrying out software decoding of the digital contest ****** transmitted from DVC13 on the IEEE1394 serial bus 200 by the CPU module 111 is explained.

[0039] First, device authentication is performed between DVC13 and the CPU module 111, and it checks mutually that it is the just device which has a copy protection function mutually. This device authentication can realize combination of for example, the random challenge & response technique, and the technique of using a strange key, when changing each time using the technique and random numbers which used the 1 orientation function or these technique etc. using the technique learned well.

[0040] A system ID is used about authentication of whether to be that to which the device of a communications partner can treat the modality of what contents. This system ID is embedded at a circuit or a firmware of each functional module in 1394 devices and PC11 etc., and it is distinguished [that a copy is possible once or] whether it is the device which can treat the digital contents of all the modalities of a copy good, copy improper, and copy free-lancer once by this, or it is the device which can treat only a copy free-lancer's digital contents.
[0041] By this authentication processing, the CPU module 111 performs key exchange with DVC13, and generates the key for canceling the encryption of the enciphered contents. Since the authentication section is in the CPU module 111, the information for generating the key itself or it is transmitted to the CPU module 111 from DVC13 through 1394 buses 200 and PCI bus 100, while it had been enciphered by it.
[0042] DVC13 enciphers a digital contents and sends it to the CPU module 111. The enciphered contents reaches the CPU module 111 through 1394 bus 200 and PCI bus 100, while it had been enciphered by it, and the decode section (De-cipher) 1112 of the CPU module 111 solves the encryption of a contents using the key obtained by authentication. When the authentication section and the decryption section of the CPU module 111 are realized by software, of course, it is necessary to devise the means which do not alter or understand an algorithm for this software.
[0043] After the contents which had the encryption solved is decoded by the software MPEG 2 decoder (Decoder) 1113 in the CPU module 111, it is sent and reproduced by the VGA controller 114 through AGP (AcceleratedGraphics Port) which ties main memory 112 and the VGA controller 114 directly.
[0044] Among the interface section of two or more functional modules of each treating a digital contents, thus, the authentication processing section, When encryption or the decryption section is prepared and digital contest ****** for a copy protection is delivered between functional modules or between a functional module and 1394 devices By performing authentication processing and encryption / decryption processing of a digital contents among these devices While the key and digital contents for encryption cancel had been enciphered also in which of IEEE1394 bus 200 and PCI bus 100, it comes to be transmitted, and the illegal copy of a digital contents can be prevented.

[0045] Moreover, since authentication processing can be performed for every functional module in PC11, it is enabled to restrict efficiently the modality (only 1 time a copy good, copy improper, a copy free-lancer) of digital contents which can be treated per functional module.
[0046] The relation of the software and hardware in the system of drawing 1 is shown in drawing 2 . In drawing 2 , the alternate long and short dash line bottom is software, and the bottom is hardware. Moreover, the blocks of **** which are hierarchized by lengthwise and shown in it are hardware devices, such as each functional module in PC11, or 1394 devices.
[0047] Authenticator handler performs authentication processing and the control for key exchange between each required hardware device according to the demand from application programs, such as software for digital contents regeneration. Since 1394 bridges 117 connect each functional module in PC11, and 1394 devices transparent as mentioned above, it is enabled to treat them equivalent from an application program by mounting the same authentication as 1394 devices, and encryption/decryption protocol in each functional module in PC11, without distinguishing each functional module in PC11, and 1394 devices as shown by the dotted line.
[0048] An example of the procedure of the authentication processing and key exchange which are used with this operation gestalt is shown in drawing 3 . The device of the side which transmits a contents is Source. The device of the side which Devices and receives is Sink. It is Device.
[0049] Sink The random challenge key (Na) which changes each time using random numbers and to replace is generated first, and Device is Source about the random challenge key (Na) in an authentication demand. Device is passed. And Sink Device creates Ar from Na using the decided function.
[0050] Source Device generates the random challenge key (Nb) which changes each time using random numbers and to replace, and returns it to SinkDevice as a response to an authentication demand. And Source Device creates Br from Nb using the decided function.

[0051] Then, Source Device is Sink about a message (Bv). It sends to Device. This message (Bv) is created from a public key, and Na and Br.
[0052] Sink Device is Source about a message (Av). It sends to Device. A message (Av) is created from a public key, and Nb and Ar.
[0053] Source Device checks whether Av is right, and if right, a partner will judge it to be a just device and it will make an authentication key (Ak). Similarly, it is Sink. It checks whether Bv is right, Device is right, and a partner judges that it is a just device and it makes an authentication key (Ak).
[0054] Then, Source Device is Sink about the control key (eKx) enciphered with the authentication key (Ak). It sends to Device. Sink Device cancels an encryption for the enciphered control key (eKx) with an authentication key (Ak), and makes a control key (Kx).
[0055] In addition, the procedure of authentication processing of drawing 3 is an example to the last, and if it can verify mutually that a mutual device is the right device mutually, as mentioned above, the usual random challenge & response technique and the technique which others are good and was learned can be used.
[0056] Next, how to restrict the contents which can be treated when the modality (a 1 time copy good, copy improper, copy free-lancer) of digital contents transmitted changes to real time for every device is explained.
[0057] The device which can transmit copy improper and the contents once which can be copied prepares separately two kinds of control keys for copy good (key which solves encryption of a contents encryption cancel key) the object for copy improper, and once, and changes the number of the control keys passed to it according to the capacity of the device of a receiving side. Moreover, when the device of a receiving side can treat both contentss (a copy is possible copy improper and once), authentication is performed twice, and both control keys are acquired beforehand. In the device of a transmitting side, although it is natural to change a key according to the modality of contents, it can correspond to a dynamic change of the modality of contents flexibly by making both keys prepare beforehand a receiving side by authentication processing.
[0058] Hereafter, an example of the concrete procedure of this authentication processing is explained with reference to the flow chart of drawing 4 . First, the following processings are performed for every device of the receiving side used as the sending place of a digital contents. First, a system ID is acquired from the device of a receiving side. And based on the system ID, it judges whether the receiving-side device can treat a copy improper contents (step S101). If a receiving-side device is a device which can treat a copy improper contents, the control key (eKcontrol#1) for [copy improper] contentss will be transmitted from a transmitting-side device to a receiving-side device, and a receiving-side device will receive the control key (eKcontrol#1) for [copy improper] contentss (step S102). To the device which cannot treat a copy improper contents, sending of the control key for [copy improper] contentss is not performed.
[0059] Next, based on a system ID, the receiving-side device judges whether the contents once which can be copied can be treated (step S103). If a receiving-side device is a device which can treat the contents once which can be copied, the control key (eKcontrol#2) for copy good contentss will be transmitted once from a transmitting-side device to a receiving-side device, and a receiving-side device will receive the control key (eKcontrol#2) (step S104). To the device which cannot treat a copy good contents once, sending of the control key for copy good contentss is not performed once.
[0060] Each [these] control key (eKcontrol#1, #2) enciphers the key for canceling encryption of the contents key enciphered as having mentioned above, and when random numbers etc. are used, it can use a strange key. In the device of a receiving side, encryption of eKcontrol#1 and #2 is solved using the random-numbers value and other keys currently beforehand prepared in the device delivered and received by authentication processing, and Kcontrol#1 and #2 are obtained.
[0061] Thus, the key according to the function of the device is passed for every receiving-side device. That is, in the case of the device which can treat the contents of both copy improper and once which can be copied, both control keys are passed by two authentications. Moreover, in the case of the device which can treat only the contents once which can be copied, only the control key

for copy good contentss will be passed once.
[0062] An end of authentication processing with all receiving-side devices carries out broadcasting sending of the contents (Encrypted contents) enciphered as the enciphered contents key (eKcontent) from a transmitting-side device at all receiving-side devices (steps S106 and S107). (step S105) Copy improper and the copy control information (CGMS) which shows a copy good or a copy free-lancer once are embedded at the header unit of the enciphered contents (Encrypted contents).
[0063] Each device of a receiving side uses a copy control information (CGMS) as contents identification information for changing a control key dynamically. That is, each device of a receiving side distinguishes the modality of contents under present reception according to the copy control information (CGMS) included in the enciphered contents, and chooses the control key (Kcontrol) corresponding to the modality of the contents. And the contents key (Kcontent) for canceling encryption of the enciphered contents key (eKcontent) and canceling encryption of the enciphered contents (Encrypted contents) is generated by using the selected control key (step S108). About the device of the receiving side which received the contents of the modality which cannot be treated, since there is no corresponding control key (Kcontrol), encryption of the contents cannot be canceled.
[0064] Thus, when transmitting the stream which consists of two or more sorts of contentss from which a modality is different with this operation gestalt, only the number of modalities of the contents which the device of a receiving side can treat performs authentication processing, and processing in which the key for encryption cancel corresponding to the number of modalities of the contents which can process the device of a receiving side in the modality of contents which constitutes a stream is passed to the device of the receiving side is performed.
[0065] Here, the case where encryption substream B which consists of encryption substream A and the contents which cannot be copied which consists of a contents once which can be copied as shown in drawing 5 is transmitted continuously is assumed.
[0066] As shown in drawing 6 , the contents identification information which shows the modality of ******** is embedded as an information for directing change of the key to use at each header unit of each encryption substreams A and B. As this contents identification information, as mentioned above, a copy control information (CGMS) can be used.
[0067] When transmitting to the device (device #1) which can treat the contents of both copy improper and once which can be copied for such an encryption stream, and the device (device #2) which can treat only the contents once which can be copied, or a copy free-lancer's contents, about device #1, encryption substream A and the encryption cancel key of both B will be passed, and only the encryption cancel key of encryption substream B will be passed about device #2.
[0068] Therefore, when the modality of contents changes from encryption substream A to encryption substream B, device #1 can obtain the right decode data (plaintext) corresponding to encryption substream A and each B by changing an encryption cancel key dynamically according to it, as shown in drawing 7 (a). On the other hand, since device #2 do not have a key for canceling encryption of encryption substream B, although they can obtain the decode data (plaintext) corresponding to encryption substream A, they cannot cancel the encryption about encryption substream B, as shown in drawing 7 (b).
[0069] In addition, although the control key according to the function of the device was passed for every receiving-side device, since it is important to make the contents key according to the function of the device prepare for every receiving-side device, various technique can be used by the technique of authentication processing used as a procedure for it here. Moreover, the configuration which prepares the authentication section and encryption/decryption section for every functional module is applicable to various microcomputer application equipments, such as a player for picture recording/regeneration of for example, not only PC but a digital contents.
[0070] Next, with reference to drawing 8 , how to record a contents on a storage device in PC11 of drawing 1 is explained. Since an authentication function generally is not prepared in the storage device used as auxiliary memory in a personal computer, a copy protection cannot record a required contents. Moreover, although it is enabled to record on a storage device after canceling

encryption of a contents, if an authentication function and a decryption function are prepared, when it does in this way, there is risk of the content (Plain Contents) of record being used unjustly shortly. In the case of the removable storage device which uses a portability type archive medium especially, the risk is high.

[0071] Then, with this operation gestalt, only the authentication processing section (Authenticator) is prepared in a storage device, and while recording on an archive medium, with a contents enciphered, it is made to record the contents key further generated by authentication on the field on the archive medium which a system cannot access.

[0072] The case where a copy protection receives the digital contents once [required] which can be copied from STB12, and records on DVD-RAM media of the DVD-RAM drive 116 hereafter is illustrated, and the record technique is explained concretely.

[0073] 1. STB12 and the DVD-RAM drive 116 -- if authentication between these devices is performed and it is checked using each authentication section (Authnticator) 121 and 1161 that it is a just device mutually, an encryption will be solved for the control key (eKcontrol) enciphered and sent from STB12 side by the DVD-RAM drive 116 side, and a control key (Kcontrol) will be generated

[0074] 2. It is sent to the DVD-RAM drive 116 with the digital contents as which the contents key (ekcontent) enciphered from STB12 was enciphered.

[0075] 3. The copy control information (CGMS) is included in the enciphered digital contents.

4. The DVD-RAM drive 116 generates a contents key (Kcontent) from eKcontent using Kcontrol and CGMS. eKcontent -- the time -- a strange key -- it is .

[0076] 5. The encryption contents (Encrypted Contents) enciphered by Kcontent is recorded on a media as it is, and corresponding Kcontent is recorded on the gap field between sectors, as shown in drawing 9 . Moreover, the content of CGMS is changed into the status "a copy is improper more than this", from "a 1 time copy is possible", and is similarly recorded on this gap field. This gap field is a field which cannot be accessed from a system.

[0077] In addition, all of control of these procedures are performed by the CPU module 111. Next, the case where the encryption contents (EncryptedContents) recorded on DVD-RAM media is reproduced with reference to drawing 10 is explained.

[0078] 1. Attest between the DVD-RAM drive 116 and the MPEG 2 decoder 115.

2. Authentication of that it is a just device mutually sends the enciphered control key (eKcontrol) to the MPEG 2 decoder 115 from the DVD-RAM drive 116.

[0079] 3. Encryption of eKcontrol is solved by Authenticator1151 in the MPEG 2 decoder 115, and Kcontrol is made.

4. The contents key (ekcontent) and CGMS which were simultaneously enciphered as the encryption contents (Encrypted Contents) are sent to the MPEG 2 decoder 115 from the DVD-RAM drive 116.

[0080] 5. Solve encryption of Kcontrol and CGMS to eKcontent by Authenticator1151 of the MPEG 2 decoder 115, and generate Kcontent.

[0081] 6. Send Kcontent to De-Cipher1152 in the MPEG 2 decoder 115.

7. De-Cipher1152 solves encryption of an encryption contents (Encrypted Contents) by the contents key, and generates PlainText of the contents.

[0082] 8. After the MPEG 2 decoder 115 decodes PlainTxet, send it to the video input port of the VGA controller 114, and it carries out a screen display of it. As mentioned above, the contents which has not been recorded and in which a 1 time copy is possible can be recorded now on a storage device until now by preparing Authenticator section for device authentication in the bus-interface section of a storage device, and recording the sent encryption contents as it is. Moreover, the decryption circuit for contents encryption cancel becomes unnecessary by recording the sent contents as it is. Moreover, only a just device becomes possible [performing encryption cancel of the content of storage of the storage device by authentication with a storage device] by writing the contents encryption cancel key by which encryption cancel was carried out in the field which cannot be read from a system.

[0083] Moreover, the digital contents enciphered in this way is recorded on a usual field, and the

key for the encryption cancel may be made to distribute various titles from a system using the record medium which is recorded on the field which is not read and made and in which computer reading is possible. It is enabled for it to become impossible to reproduce the content of the record medium only by the just device with authentication and encryption/decryption function by this, and to prevent an illegal copy.

[0084] In addition, although DVD-RAM drive was illustrated as a storage device, you may apply to DVD-R drive, MO drive, HDD, etc. here. Moreover, the storage device which has an authentication function in this way is applicable to the various microcomputer application equipments which use the storage device in which read/write is possible, such as a compound machine of for example, not only PC but DVD player, and D-VCR. Moreover, of course, you may realize as IEEE1394 device.

[0085] Next, the data transfer limit technique of restricting the device which can treat the contents using the attribute (a field, area) of the contents enciphered and transmitted is explained.

[0086] That is, although how to restrict until now copy improper and the device which can treat it once based on the copy control information of copy-izing and a copy free-lancer was explained, this technique is the control which made the unit fundamentally the whole stream which consists of a contents of the same modality. Therefore, it is difficult to perform fine control of enabling it to treat only the fraction to which treating suited some specific conditions in the contents of the allowed modality.

[0087] Then, by embedding the field information and the local information which show the content of a contents by this data transfer limit technique at the header unit of stream data, and using these fields information and a local information In the stream which treating becomes from the contents of the allowed modality (only 1 time copy improper, copy-izing or a copy free-lancer) Processing of only the fraction which suits the conditions (a field, area) specified beforehand is enabled, and it is preventing from processing about other other fractions by the user etc.

[0088] The system configuration for realizing this data transfer limit technique is shown in drawing 11 . First, the transfer control according to the field information added to the bucket header unit of stream data is explained.

[0089] A "field" here means the sort of the existence and the grade of sexual depiction, existence, a grade of violent depiction, etc., etc. demanded socially and educationally. It is stream data at the transit time of a network path, they are packet-ized, and this packet consists of the header unit and the data itself with the information on data. In addition, it does not matter even if it is a part for the header unit which data connote even if a header unit here is an HDR which a network path specifies.

[0090] The data output system 301 consists of the interface section 303 which outputs the stream data-storage equipment 302 and it outside. Here, the data packet which should be outputted to a network path is created. The information on a "field" is stored in the header unit of the packet as shown in drawing 12 . A network does not ask the exception of a cable and a radio. Moreover, you may be the IEEE1394 serial bus 200, PCI bus 100, etc. of drawing 1 .

[0091] Data processing system 401 is in the equipment which receives stream data. For example, in PC11 of drawing 1 , a tuner 113, the CPU module 111, or the MPEG 2 decoder 115 will be equivalent to data processing system 401. Moreover, data processing system 401 may be 1394 devices of not only PC but drawing, and may be a satellite terminal and an internet terminal.

[0092] Data processing system 401 is the fraction which performs processing for actually showing an user data, and consists of the stream data-processing section 403 processed with the interface section 402 which receives data. That is, a "field" information is decoded to the timing which processes not the time of receiving data but the data itself, and the propriety of processing of the data is determined per data packet by the comparison with the field defined by the system attribute information beforehand set up by the user of data processing system 401 etc.

[0093] In addition, only the hardware of the interface section is [any of both joint field] sufficient only as software. Moreover, you may be made to embed the "local" information for pinpointing the area which can process not only a "field" information but the contents which adds to instead of [the] or it, and corresponds to stream data. Here, according to an intention of the implementor of

stream data or a distribution person, it is classified with an "area." Also in this case, a "local" information is decoded to the timing which processes not the time of receiving data but the data itself, and the propriety of processing of the data is determined per data packet by the comparison with the area specified by the system information of data processing system 401.

[0094] A mode that the propriety of processing of data is controlled by the stream attribute informations embedded at the packet HDR of a stream, such as a "field" and an "area", is shown in drawing 13 .

[0095] In drawing 13 , the digital contents of the modality which can be treated by data processing system 401 consists of data packets A, B, C, and D, and the case where the "field" or the "local" information is included in the header unit as a stream attribute information for every data packet is shown.

[0096] Only the data (data A, data C) of the "field" which suits data processing system 401, or an "area" are processed, and other data (data B, data D) are excepted from a processing object, and are discarded by the stream limit function of data processing system 401. Processing of a stream limit function is performed by the procedure shown in the flow chart of drawing 14 . That is, the system attribute information set as data processing system 401 is acquired first, and the comparison with the stream attribute information included in the received packet HDR of a stream is performed (steps S201-S204). If in agreement, processing of the stream (packet) is performed (step S205), and it will not be processed if inharmonious (step S206).

[0097] Therefore, when [of drawing 1] the stream limit function of data processing system 401 is added to the MPEG 2 decoder 115 In the picture contents (data A, B, C, and D) transmitted continuously Only the data (data A, data C) corresponding to a "field" or an "area" of an user setup are decoded and reproduced, and the decoding and regeneration are not performed about other data (data B, data D). That is, data C will be reproduced, after reproducing data A, and the regeneration term of data B serves as a blanking and the regeneration term of data B finishes.

[0098] Therefore, fine control of only the scene which agreed on each user's conditions by applying the system configuration of drawing 11 to the contents offer system against many and unspecified persons like a satellite TV broadcast being reproducible, or enabling it to record and enabling it to treat only the fraction to which treating suited some specific conditions in the contents of the allowed modality can be easily realized now.

[0099]

[Effect of the Invention] As explained above, according to this invention, protection of the digital contents which flows on the bus which connects between functional modules, and a limit of the digital contents in a functional-module unit can be efficiently realized now by preparing the authentication function for encryption processing in each functional module which constitutes data processors, such as a personal computer.

TECHNICAL FIELD

[The technical field to which invention belongs] this invention relates to the copy protection technique applied to the data processor which has an interface with external buses, such as an IEEE1394 serial bus, especially, and this equipment about the copy protection technique of the digital contents used with a data processor and these equipments, such as a personal computer.

PRIOR ART

[Description of the Prior Art] In recent years, in connection with development of computer technique, the electronic equipment of multimedia correspondence, such as a digital video player, a set top box, TV, and a personal computer, is developed variously.

[0003] This kind of electronic equipment can reproduce digital contentss, such as TV program by the movie and digital satellite broadcasting which were accumulated at DVD (Digital VersatileDisk).

[0004] A digital contents is sent to each home through a record medium and a transmission medium, after encoding generally using a dynamic-image bandwidth compression method called MPEG 2. Coding by MPEG 2 is based on the idea of a viewpoint to adjustable rate coding which secures quality of image and the both sides of a chart lasting time to capacity. In the amount of data of adjustable rate coded data, depending on the quality of image of the original picture image, the amount of data increases the more intense scene of a motion. Therefore, a digital contents can offer the high-definition picture which does not have an original picture and inferiority in each home.

[0005] The present condition is that effective technique is not built from viewpoints, such as copyright protection of such a digital contents, in recent years although cried for the need for the copy protection technique for preventing the illegal copy.

[0006] Then, in CPTWG (Copy Protection TechnicalWorking Group), decision work of the specification (IEEE1394 copy-protection technique is called hereafter) of the new copy protection method towards the IEEE1394 serial bus which is the bus interface of the suitable next generation for a transmission of multimedia data is done.

[0007] It is the bus interface of the next generation which connects a digital video player, a set top box, TV, a personal computer, etc., and an IEEE1394 serial bus is a ****** clo eggplant as transfer mode. As isochronous as a sub action Two kinds of sub actions are supported. The former is called Asynchronous Transfer Mode and used at the time of the general data transfer as which real time nature is not required. The latter is the synchronous transfer mode which guaranteed the transfer band, and the real-time transfer of the digital contents represented by a video data and audio data is possible for it.

[0008] IEEE1394 copy-protection technique enciphers the digital contents delivered through an IEEE1394 serial bus among devices, such as a digital video player, a set top box, TV, and a personal computer, and enables it to prevent the illegal copy by using the encryption protocol which a public-key-encryption-ized method, a common key cipher system, etc. are good, and was known.

EFFECT OF THE INVENTION

[Effect of the Invention] As explained above, according to this invention, protection of the digital contents which flows on the bus which connects between functional modules, and a limit of the digital contents in a functional-module unit can be efficiently realized now by preparing the authentication function for encryption processing in each functional module which constitutes data processors, such as a personal computer.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] However, since a personal computer is a system open from the first, it cannot expect sufficient protection to an illegal copy only by enciphering the data which flow on an IEEE1394 serial bus. Hereafter, this is explained concretely.

[0010] Drawing 15 is an example of a configuration at the time of applying IEEE1394 copy-protection technique to a personal computer as it was. In drawing 15 , a mode that a personal computer (PC) 1, the set top box (STB) 2, and three devices of a digital camcorder (DVC) 3 are connected through the IEEE1394 serial bus 10 is shown.

[0011] These personal computers (PC) 1, the set top box (STB) 2, and the digital camcorder (DVC) 3 have the encryption section (Cipher), the decryption section (De-Cipher), or encryption/decryption section (De-/Cipher) with both function of encryption and a decryption among the interface section with the IEEE1394 serial bus 10, respectively.

[0012] namely, -- IEEE -- 1394 -- serial -- a bus -- ten -- minding -- others -- a device -- digital -- a contents -- sending -- carrying out -- a digital camcorder (DVC) -- three -- ******** -- encryption -- the section (Cipher) -- preparing -- having -- IEEE -- 1394 -- serial -- a bus -- ten -- minding -- others -- a device -- between -- digital -- a contents -- transmission and reception -- carrying out -- a personal computer -- (-- PC --) -- one -- and -- a set top box (STB

[0013] The digital contents which needs a copy protection is outputted on the IEEE1394 serial bus 10, after enciphering by the device of the transmitting side, the encryption data is decrypted by the device of a receiving side, and encryption is canceled. Thus, by enciphering the data which flow on the IEEE1394 serial bus 10, even if the data which flow on the IEEE1394 serial bus 10 are copied unjustly, it can prevent that it will be reproduced normally.

[0014] In a personal computer (PC) 1, encryption/decryption section (De-/Cipher) is prepared like illustration in 1394 bridges 6 which connect between system buses, such as PCI bus 20, and the IEEE1394 serial buses 10 with both directions. Thereby, since encryption data do not flow, but it usually passes on PCI bus 20 and only plaintext data flow, open bus architecture is maintainable.

[0015] After the encryption data transmitted to a personal computer (PC) 1 through the IEEE1394 serial bus 10 from the digital camcorder (DVC) 3 or the set top box (STB) 2 are decrypted by 1394 bridges 6 at a plaintext, they are sent to CPU4 and the MPEG decoder 5 on PCI bus 20. When transmitting a digital picture contents to a set top box (STB) 2 from CPU4 or the MPEG decoder 5, after the plaintext on PCI bus 20 is similarly enciphered by 1394 bridges 6, it delivers on the IEEE1394 serial bus 10.

[0016] Thus, if encryption/decryption function is prepared in 1394 bridges 6, although the open architecture of PCI bus 20 is maintainable as it is, the data (Plain Contents) with which encryption was solved by PCI bus 20 will flow, and a copy will become possible easily.

[0017] Moreover, in the personal computer of the drawing 15 which prepared encryption/decryption function in 1394 bridges 6, it becomes difficult to perform control of restricting the modality (only 1 time a copy good, copy improper, a copy free-lancer) of contents which constitutes a personal computer and which the functional module can treat for every functional module. For example, it is necessary for storage devices, such as DVD-RAM and HDD, to be able to treat only the contents once which can be copied, and a copy free-lancer's contents, and for things to be made not to be made to enabling it to treat the contents (only 1 time a copy good, copy improper, a copy free-lancer) of all modalities about MPEG 2 decoder. However, it is Plain to PCI bus 20. If Contents flows, it is difficult to restrict the contents which it can treat for every functional module in practice. It is because such a limit of a contents is usually performed by authentication processing between devices. That is, when encryption/decryption function is prepared in 1394 bridges 6, a personal computer is also treated as one device on an IEEE1394 serial bus. For this reason, although it is possible to restrict the modality of contents which can treat the personal computer by authentication processing between a personal computer and other devices on an IEEE1394 serial bus, the modality of contents cannot be restricted per each module in a personal computer.

[0018] Moreover, in DVD video etc., the digital contents is realized in many cases as a stream containing two or more contentss from which a modality is different. In this case, although the

modality of contents for regeneration will change dynamically, in having done authentication again, whenever the modality of contents changed, there is also a problem that it becomes impossible to process a contents on real time.

[0019] this invention is made in view of the above-mentioned actual condition, and it enables it to realize protection of the digital contents which flows on the bus in data processors, such as a personal computer, and a limit of the digital contents in the functional-module unit which constitutes a data processor, and aims at offering the copy protection technique applied to the data processor which can perform the copy protection of a digital contents efficiently, and this equipment.

MEANS

[Means for Solving the Problem] In the data processor which has an interface with the external bus which can connect the external instrument which has an authentication function for this invention enciphering, delivering and receiving the data for a copy protection in order to solve an above-mentioned technical probrem An internal bus and two or more functional modules which are combined with this internal bus, respectively, and transmit or receive the data for a copy protection via [aforementioned] an internal bus, Between the functional modules of the partner point or the aforementioned external instruments which are prepared for every aforementioned functional module, and deliver and receive the data for [aforementioned] a copy protection An authentication means to perform authentication processing for enciphering, delivering and receiving the data for [aforementioned] a copy protection is provided, and it is characterized by performing authentication processing for every functional module in the aforementioned data processor.

[0021] In this data processor, the authentication means is prepared in the interface section of two or more functional modules of each treating the data for [, such as a digital contents,] a copy protection, and authentication processing is individually performed between functional modules or between a functional module and an external instrument. Therefore, on the internal bus to which these functional modules were connected, the key and digital contents for encryption cancel come to be transmitted while it had been enciphered by them, and they can prevent the illegal copy of a digital contents. Moreover, since authentication processing is performed for every functional module, it is enabled to restrict efficiently the modality (only 1 time a copy good, copy improper, a copy free-lancer) of digital contents which can be treated by it per functional module.

[0022] Moreover, it is enabled to enable it to use the same authentication and an encryption protocol on the both sides between [aforementioned] functional modules and between the aforementioned external instrument and the aforementioned functional module by providing further an external bus interface means to connect between the external bus which can connect the external instrument which has the data encryption / decryption function for a copy protection, and the buses in the aforementioned data processor transparent. That is, it is enabled to treat similarly, without distinguishing the functional module and external instrument in a data processor, if it sees from each functional module or application program in a data processor.

[0023] The data once which can be copied, and the data which cannot be copied are in the modality of data for [aforementioned] a copy protection. moreover, to each aforementioned functional module The identification information for specifying the modality of data which can process the functional module is assigned. the aforementioned authentication means It is desirable to distinguish whether it is a functional module with the functional module of the aforementioned sending place able to treat the data for [aforementioned] sending based on the modality of data for sending and the identification information (system ID) of the functional module of a sending place.

[0024] Thus, by using a system ID, it is enabled to manage easily the modality of digital contents which can be treated per functional module. Moreover, as for an encryption cancel key required in order to decrypt the enciphered data, it is desirable to change for every (for a copy good and a copy to be impossible once) modality of data for sending. When this notifies only the key according to the contents which can treat it to each functional module for example, at the time of authentication processing, even if it is the case where the broadcasting transfer of the encryption contents is carried out at two or more functional modules, it is enabled to restrict so that only the functional module which can treat the contents can perform the decode.

[0025] Moreover, when transmitting the stream which consists of two or more sorts of data with which a modality is different, as for the aforementioned authentication means, it is desirable to notify the encryption cancel key corresponding to the number of modalities of the data which can process the functional module of a sending place in the modality of data with which only the number of modalities of the contents which the functional module of a sending place can treat performs authentication processing, and constitutes the aforementioned stream to the functional module of the aforementioned sending place. Thus, even if the modality of contents is dynamically

changed by passing the encryption cancel key for every modality of contents beforehand to the functional module of a receiving side, it is enabled to cancel encryption on real time. In this case, the data class information which shows the modality of data is embedded at the stream, and a decryption means should just change dynamically the encryption cancel key used for decryption processing based on the aforementioned data class information.

[0026] Moreover, this invention is set to the data processor which transmits data to a receiving set side so that the unjust copy of the digital contents passed on an internal bus may be prevented. An authentication means to attest whether processing of the data for a copy protection is permitted between the aforementioned receiving sets, A judgment means by which the data for a copy protection with which processing is permitted to the aforementioned receiving set distinguish what kind of digital contents it is when attested by the aforementioned authentication means, A key transmitting means to transmit the encryption cancel key corresponding to the modality of digital contents by which processing is permitted to the aforementioned receiving set to the aforementioned receiving set based on the judgment result of this judgment means, respectively, The aforementioned receiving set is characterized by providing a transmitting means to transmit the digital contents which can cancel an encryption using the aforementioned encryption cancel key.

[0027] In this data processor, it is attested whether processing of the data for a copy protection is permitted between the aforementioned receiving sets. When attested, the data for a copy protection with which processing is permitted to the aforementioned receiving set Only the encryption cancel key corresponding to the modality of digital contents by which it is distinguished what kind of digital contents it is, and processing is permitted to the aforementioned receiving set based on this judgment result is transmitted to the aforementioned receiving set, respectively. And the digital contents of which the aforementioned receiving set can cancel an encryption using this encryption cancel key is transmitted to a receiving set.

[0028] Moreover, this invention is set to the data processor which carries out reception of the data transmitted from the sending set side so that the illegal copy of the digital contents passed on an internal bus might be prevented. An authentication means to attest whether processing of the data for a copy protection is permitted between the aforementioned sending sets, A modality information transmitting means to transmit the information which shows the modality of digital contents for [by which processing is permitted to this data processor] a copy protection when attested by the aforementioned authentication means to the aforementioned sending set, The encryption cancel key respectively corresponding to the modality of digital contents for [by which processing is permitted to the aforementioned data processor based on this modality information] a copy protection, The digital contents of which the aforementioned data processor can cancel an encryption using this encryption cancel key is received from the aforementioned sending set, and it is characterized by providing a decryption means to decrypt the aforementioned digital contents.

[0029] In this data processor, it is attested whether processing of the data for a copy protection is permitted between the aforementioned sending sets, and when attested, the information which shows the modality of digital contents for [to which the reception of data is permitted] a copy protection is transmitted to the aforementioned sending set. And based on a modality information, the encryption cancel key corresponding to the modality of digital contents to which the aforementioned reception is permitted is received from the aforementioned sending set, respectively, and the digital contents of which a receiving set can subsequently cancel an encryption using this encryption cancel key is received from the aforementioned sending set. And the aforementioned digital contents is decrypted using the aforementioned encryption cancel key.

[0030]

[Embodiments of the Invention] Hereafter, the operation gestalt of this invention is explained with reference to a drawing. The system configuration of the personal computer (PC is called hereafter) concerning the 1 operation gestalt of this invention is shown in drawing 1 . this -- PC -- 11 -- IEEE -- 1394 -- serial -- a bus -- 200 -- minding -- the exterior -- consumer -- electronic equipment -- for example, -- illustration -- like -- a set top box (STB) -- 12 -- a digital camcorder -- or -- DV -- a camcorder (DVC) -- 13 -- and -- digital -- a video cassette recorder (D-VCR) -- 14 -- a

communication -- possible -- constituting -- having -- **** .
[0031] The set top box (STB) 12, the digital camcorder (DVC) 13, and the digital video cassette recorder (D-VCR) 14 have the authentication processing section (Authenticator) 121,131,141 which performs device authentication, key exchange, etc. among the interface section with the IEEE1394 serial bus 200, in order to support IEEE1394 copy-protection technique, respectively. About the set top box (STB) 12 and the digital video cassette recorder (D-VCR) 14 which transmit and receive a digital contents, encryption/decryption section (De-/Cipher) 122,142 with both function of encryption and a decryption is formed. Moreover, only the encryption section (Cipher) 132 is formed about the digital camcorder (DVC) 13 which performs only sending of a digital contents.
[0032] The IEEE1394 serial bus 200 top is transmitted to the digital contents delivered and received between PC11, the set top box (STB) 12, the digital camcorder (DVC) 13, and the digital video cassette recorder (D-VCR) 14 in the status that it was enciphered.
[0033] PC11 consists of PCI bus 100 and two or more functional modules connected to this like illustration. In these functional modules, the authentication processing sections (Authenticator) 1111, 1131, 1151, and 1161 which perform device authentication, key exchange, etc. among the interface section with PCI bus 100 are formed about the tuner 113 for the functional module 111 treating digital contest ******, i.e., CPU module, a satellite, or digital TV, the MPEG 2 decoder 115, and the DVD-RAM drive 116. The function of each [these] authentication processing sections (Authenticator) 1111, 1131, 1151, and 1161 performs authentication required [it is the same as that of it of the set top box (STB) 12 which is 1394 devices, the digital camcorder (DVC) 13, and the digital video cassette recorder (D-VCR) 14 fundamentally, and] in order to encipher, deliver and receive a digital contents, and key exchange.
[0034] Moreover, the decryption section (De-cipher) which performs decryption processing for canceling encryption of the enciphered contents (encrypted contents) further, or the encryption section (Cipher) is prepared in the interface section of these CPUs module 111, the tuner 113, and the MPEG 2 decoder 115. It is decided by the function of each functional module whether it has the decryption section with the encryption section or it has the both. Here, the case where the encryption section (Cipher) 1132 is formed about a tuner 113, and the decryption sections (De-cipher) 1112 and 1152 are formed about the CPU module 111 and the MPEG 2 decoder 115 is illustrated.
[0035] The CPU module 111 consists of a microprocessor, a memory controller, PCI bus bridge, etc., and the authentication section 1111 and the encryption cancel section 1112 can be incorporated as for example, a part of PCI bus bridge. Moreover, software may realize the authentication section 1111 in the CPU module 111, the encryption cancel section 1112, and MPEG 2 decoder section 1113.
[0036] The DVD-RAM drive 116 is formed as auxiliary memory of PC11, and is connected to PCI bus 100 through IDE interface or ATAPI interface. The DVD-RAM drive 116 has only the authentication processing section 1161, and is not prepared about the decryption section (De-cipher) and the encryption section (Cipher). It is for recording on DVD-RAM116 with the status that the enciphered digital contents was enciphered.
[0037] 1394 bridges 117 which connect between PCI bus 100 and the IEEE1394 serial bus 200 in both directions are further established in PC11. No authentication processing sections, encryption sections, and decryption sections are prepared in 1394 bridges 117, but it passes through the enciphered digital contents IEEE1394 serial bus 200 from PCI bus 100 with the status that it was enciphered, and it is transmitted to PCI bus 100 from the IEEE1394 serial bus 200. Thus, 1394 bridges 117 connect between the functional module in PC11, and 1394 devices transparent.
[0038] Here, the procedure in the case of carrying out software decoding of the digital contest ****** transmitted from DVC13 on the IEEE1394 serial bus 200 by the CPU module 111 is explained.
[0039] First, device authentication is performed between DVC13 and the CPU module 111, and it checks mutually that it is the just device which has a copy protection function mutually. This device authentication can realize combination of for example, the random challenge & response

technique, and the technique of using a strange key, when changing each time using the technique and random numbers which used the 1 orientation function or these technique etc. using the technique learned well.

[0040] A system ID is used about authentication of whether to be that to which the device of a communications partner can treat the modality of what contents. This system ID is embedded at a circuit or a firmware of each functional module in 1394 devices and PC11 etc., and it is distinguished [that a copy is possible once or] whether it is the device which can treat the digital contents of all the modalities of a copy good, copy improper, and copy free-lancer once by this, or it is the device which can treat only a copy free-lancer's digital contents.

[0041] By this authentication processing, the CPU module 111 performs key exchange with DVC13, and generates the key for canceling the encryption of the enciphered contents. Since the authentication section is in the CPU module 111, the information for generating the key itself or it is transmitted to the CPU module 111 from DVC13 through 1394 buses 200 and PCI bus 100, while it had been enciphered by it.

[0042] DVC13 enciphers a digital contents and sends it to the CPU module 111. The enciphered contents reaches the CPU module 111 through 1394 bus 200 and PCI bus 100, while it had been enciphered by it, and the decode section (De-cipher) 1112 of the CPU module 111 solves the encryption of a contents using the key obtained by authentication. When the authentication section and the decryption section of the CPU module 111 are realized by software, of course, it is necessary to devise the means which do not alter or understand an algorithm for this software.

[0043] After the contents which had the encryption solved is decoded by the software MPEG 2 decoder (Decoder) 1113 in the CPU module 111, it is sent and reproduced by the VGA controller 114 through AGP (AcceleratedGraphics Port) which ties main memory 112 and the VGA controller 114 directly.

[0044] Among the interface section of two or more functional modules of each treating a digital contents, thus, the authentication processing section, When encryption or the decryption section is prepared and digital contest ****** for a copy protection is delivered between functional modules or between a functional module and 1394 devices By performing authentication processing and encryption / decryption processing of a digital contents among these devices While the key and digital contents for encryption cancel had been enciphered also in which of IEEE1394 bus 200 and PCI bus 100, it comes to be transmitted, and the illegal copy of a digital contents can be prevented.

[0045] Moreover, since authentication processing can be performed for every functional module in PC11, it is enabled to restrict efficiently the modality (only 1 time a copy good, copy improper, a copy free-lancer) of digital contents which can be treated per functional module.

[0046] The relation of the software and hardware in the system of drawing 1 is shown in drawing 2 . In drawing 2 , the alternate long and short dash line bottom is software, and the bottom is hardware. Moreover, the blocks of **** which are hierarchized by lengthwise and shown in it are hardware devices, such as each functional module in PC11, or 1394 devices.

[0047] Authenticator handler performs authentication processing and the control for key exchange between each required hardware device according to the demand from application programs, such as software for digital contents regeneration. Since 1394 bridges 117 connect each functional module in PC11, and 1394 devices transparent as mentioned above, it is enabled to treat them equivalent from an application program by mounting the same authentication as 1394 devices, and encryption/decryption protocol in each functional module in PC11, without distinguishing each functional module in PC11, and 1394 devices as shown by the dotted line.

[0048] An example of the procedure of the authentication processing and key exchange which are used with this operation gestalt is shown in drawing 3 . The device of the side which transmits a contents is Source. The device of the side which Devices and receives is Sink. It is Device.

[0049] Sink The random challenge key (Na) which changes each time using random numbers and to replace is generated first, and Device is Source about the random challenge key (Na) in an authentication demand. Device is passed. And Sink Device creates Ar from Na using the decided function.

[0050] Source Device generates the random challenge key (Nb) which changes each time using random numbers and to replace, and returns it to SinkDevice as a response to an authentication demand. And Source Device creates Br from Nb using the decided function.
[0051] Then, Source Device is Sink about a message (Bv). It sends to Device. This message (Bv) is created from a public key, and Na and Br.
[0052] Sink Device is Source about a message (Av). It sends to Device. A message (Av) is created from a public key, and Nb and Ar.
[0053] Source Device checks whether Av is right, and if right, a partner will judge it to be a just device and it will make an authentication key (Ak). Similarly, it is Sink. It checks whether Bv is right, Device is right, and a partner judges that it is a just device and it makes an authentication key (Ak).
[0054] Then, Source Device is Sink about the control key (eKx) enciphered with the authentication key (Ak). It sends to Device. Sink Device cancels an encryption for the enciphered control key (eKx) with an authentication key (Ak), and makes a control key (Kx).
[0055] In addition, the procedure of authentication processing of drawing 3 is an example to the last, and if it can verify mutually that a mutual device is the right device mutually, as mentioned above, the usual random challenge & response technique and the technique which others are good and was learned can be used.
[0056] Next, how to restrict the contents which can be treated when the modality (a 1 time copy good, copy improper, copy free-lancer) of digital contents transmitted changes to real time for every device is explained.
[0057] The device which can transmit copy improper and the contents once which can be copied prepares separately two kinds of control keys for copy good (key which solves encryption of a contents encryption cancel key) the object for copy improper, and once, and changes the number of the control keys passed to it according to the capacity of the device of a receiving side. Moreover, when the device of a receiving side can treat both contentss (a copy is possible copy improper and once), authentication is performed twice, and both control keys are acquired beforehand. In the device of a transmitting side, although it is natural to change a key according to the modality of contents, it can correspond to a dynamic change of the modality of contents flexibly by making both keys prepare beforehand a receiving side by authentication processing.
[0058] Hereafter, an example of the concrete procedure of this authentication processing is explained with reference to the flow chart of drawing 4 . First, the following processings are performed for every device of the receiving side used as the sending place of a digital contents. First, a system ID is acquired from the device of a receiving side. And based on the system ID, it judges whether the receiving-side device can treat a copy improper contents (step S101). If a receiving-side device is a device which can treat a copy improper contents, the control key (eKcontrol#1) for [copy improper] contentss will be transmitted from a transmitting-side device to a receiving-side device, and a receiving-side device will receive the control key (eKcontrol#1) for [copy improper] contentss (step S102). To the device which cannot treat a copy improper contents, sending of the control key for [copy improper] contentss is not performed.
[0059] Next, based on a system ID, the receiving-side device judges whether the contents once which can be copied can be treated (step S103). If a receiving-side device is a device which can treat the contents once which can be copied, the control key (eKcontrol#2) for copy good contentss will be transmitted once from a transmitting-side device to a receiving-side device, and a receiving-side device will receive the control key (eKcontrol#2) (step S104). To the device which cannot treat a copy good contents once, sending of the control key for copy good contentss is not performed once.
[0060] Each [these] control key (eKcontrol#1, #2) enciphers the key for canceling encryption of the contents key enciphered as having mentioned above, and when random numbers etc. are used, it can use a strange key. In the device of a receiving side, encryption of eKcontrol#1 and #2 is solved using the random-numbers value and other keys currently beforehand prepared in the device delivered and received by authentication processing, and Kcontrol#1 and #2 are obtained.
[0061] Thus, the key according to the function of the device is passed for every receiving-side

device. That is, in the case of the device which can treat the contents of both copy improper and once which can be copied, both control keys are passed by two authentications. Moreover, in the case of the device which can treat only the contents once which can be copied, only the control key for copy good contentss will be passed once.

[0062] An end of authentication processing with all receiving-side devices carries out broadcasting sending of the contents (Encrypted contents) enciphered as the enciphered contents key (eKcontent) from a transmitting-side device at all receiving-side devices (steps S106 and S107). (step S105) Copy improper and the copy control information (CGMS) which shows a copy good or a copy free-lancer once are embedded at the header unit of the enciphered contents (Encrypted contents).

[0063] Each device of a receiving side uses a copy control information (CGMS) as contents identification information for changing a control key dynamically. That is, each device of a receiving side distinguishes the modality of contents under present reception according to the copy control information (CGMS) included in the enciphered contents, and chooses the control key (Kcontrol) corresponding to the modality of the contents. And the contents key (Kcontent) for canceling encryption of the enciphered contents key (eKcontent) and canceling encryption of the enciphered contents (Encrypted contents) is generated by using the selected control key (step S108). About the device of the receiving side which received the contents of the modality which cannot be treated, since there is no corresponding control key (Kcontrol), encryption of the contents cannot be canceled.

[0064] Thus, when transmitting the stream which consists of two or more sorts of contentss from which a modality is different with this operation gestalt, only the number of modalities of the contents which the device of a receiving side can treat performs authentication processing, and processing in which the key for encryption cancel corresponding to the number of modalities of the contents which can process the device of a receiving side in the modality of contents which constitutes a stream is passed to the device of the receiving side is performed.

[0065] Here, the case where encryption substream B which consists of encryption substream A and the contents which cannot be copied which consists of a contents once which can be copied as shown in drawing 5 is transmitted continuously is assumed.

[0066] As shown in drawing 6 , the contents identification information which shows the modality of ******** is embedded as an information for directing change of the key to use at each header unit of each encryption substreams A and B. As this contents identification information, as mentioned above, a copy control information (CGMS) can be used.

[0067] When transmitting to the device (device #1) which can treat the contents of both copy improper and once which can be copied for such an encryption stream, and the device (device #2) which can treat only the contents once which can be copied, or a copy free-lancer's contents, about device #1, encryption substream A and the encryption cancel key of both B will be passed, and only the encryption cancel key of encryption substream B will be passed about device #2.

[0068] Therefore, when the modality of contents changes from encryption substream A to encryption substream B, device #1 can obtain the right decode data (plaintext) corresponding to encryption substream A and each B by changing an encryption cancel key dynamically according to it, as shown in drawing 7 (a). On the other hand, since device #2 do not have a key for canceling encryption of encryption substream B, although they can obtain the decode data (plaintext) corresponding to encryption substream A, they cannot cancel the encryption about encryption substream B, as shown in drawing 7 (b).

[0069] In addition, although the control key according to the function of the device was passed for every receiving-side device, since it is important to make the contents key according to the function of the device prepare for every receiving-side device, various technique can be used by the technique of authentication processing used as a procedure for it here. Moreover, the configuration which prepares the authentication section and encryption/decryption section for every functional module is applicable to various microcomputer application equipments, such as a player for picture recording/regeneration of for example, not only PC but a digital contents.

[0070] Next, with reference to drawing 8 , how to record a contents on a storage device in PC11 of

drawing 1 is explained. Since an authentication function generally is not prepared in the storage device used as auxiliary memory in a personal computer, a copy protection cannot record a required contents. Moreover, although it is enabled to record on a storage device after canceling encryption of a contents, if an authentication function and a decryption function are prepared, when it does in this way, there is risk of the content (Plain Contents) of record being used unjustly shortly. In the case of the removable storage device which uses a portability type archive medium especially, the risk is high.

[0071] Then, with this operation gestalt, only the authentication processing section (Authenticator) is prepared in a storage device, and while recording on an archive medium, with a contents enciphered, it is made to record the contents key further generated by authentication on the field on the archive medium which a system cannot access.

[0072] The case where a copy protection receives the digital contents once [required] which can be copied from STB12, and records on DVD-RAM media of the DVD-RAM drive 116 hereafter is illustrated, and the record technique is explained concretely.

[0073] 1. STB12 and the DVD-RAM drive 116 -- if authentication between these devices is performed and it is checked using each authentication section (Authnticator) 121 and 1161 that it is a just device mutually, an encryption will be solved for the control key (eKcontrol) enciphered and sent from STB12 side by the DVD-RAM drive 116 side, and a control key (Kcontrol) will be generated

[0074] 2. It is sent to the DVD-RAM drive 116 with the digital contents as which the contents key (ekcontent) enciphered from STB12 was enciphered.

[0075] 3. The copy control information (CGMS) is included in the enciphered digital contents.

4. The DVD-RAM drive 116 generates a contents key (Kcontent) from eKcontent using Kcontrol and CGMS. eKcontent -- the time -- a strange key -- it is .

[0076] 5. The encryption contents (Encrypted Contents) enciphered by Kcontent is recorded on a media as it is, and corresponding Kcontent is recorded on the gap field between sectors, as shown in drawing 9 . Moreover, the content of CGMS is changed into the status "a copy is improper more than this", from "a 1 time copy is possible", and is similarly recorded on this gap field. This gap field is a field which cannot be accessed from a system.

[0077] In addition, all of control of these procedures are performed by the CPU module 111. Next, the case where the encryption contents (EncryptedContents) recorded on DVD-RAM media is reproduced with reference to drawing 10 is explained.

[0078] 1. Attest between the DVD-RAM drive 116 and the MPEG 2 decoder 115.

2. Authentication of that it is a just device mutually sends the enciphered control key (eKcontrol) to the MPEG 2 decoder 115 from the DVD-RAM drive 116.

[0079] 3. Encryption of eKcontrol is solved by Authenticator1151 in the MPEG 2 decoder 115, and Kcontrol is made.

4. The contents key (ekcontent) and CGMS which were simultaneously enciphered as the encryption contents (Encrypted Contents) are sent to the MPEG 2 decoder 115 from the DVD-RAM drive 116.

[0080] 5. Solve encryption of Kcontrol and CGMS to eKcontent by Authenticator1151 of the MPEG 2 decoder 115, and generate Kcontent.

[0081] 6. Send Kcontent to De-Cipher1152 in the MPEG 2 decoder 115.

7. De-Cipher1152 solves encryption of an encryption contents (Encrypted Contents) by the contents key, and generates PlainText of the contents.

[0082] 8. After the MPEG 2 decoder 115 decodes PlainTxet, send it to the video input port of the VGA controller 114, and it carries out a screen display of it. As mentioned above, the contents which has not been recorded and in which a 1 time copy is possible can be recorded now on a storage device until now by preparing Authenticator section for device authentication in the bus-interface section of a storage device, and recording the sent encryption contents as it is. Moreover, the decryption circuit for contents encryption cancel becomes unnecessary by recording the sent contents as it is. Moreover, only a just device becomes possible [performing encryption cancel of the content of storage of the storage device by authentication with a storage device] by writing the

contents encryption cancel key by which encryption cancel was carried out in the field which cannot be read from a system.

[0083] Moreover, the digital contents enciphered in this way is recorded on a usual field, and the key for the encryption cancel may be made to distribute various titles from a system using the record medium which is recorded on the field which is not read and made and in which computer reading is possible. It is enabled for it to become impossible to reproduce the content of the record medium only by the just device with authentication and encryption/decryption function by this, and to prevent an illegal copy.

[0084] In addition, although DVD-RAM drive was illustrated as a storage device, you may apply to DVD-R drive, MO drive, HDD, etc. here. Moreover, the storage device which has an authentication function in this way is applicable to the various microcomputer application equipments which use the storage device in which read/write is possible, such as a compound machine of for example, not only PC but DVD player, and D-VCR. Moreover, of course, you may realize as IEEE1394 device.

[0085] Next, the data transfer limit technique of restricting the device which can treat the contents using the attribute (a field, area) of the contents enciphered and transmitted is explained.

[0086] That is, although how to restrict until now copy improper and the device which can treat it once based on the copy control information of copy-izing and a copy free-lancer was explained, this technique is the control which made the unit fundamentally the whole stream which consists of a contents of the same modality. Therefore, it is difficult to perform fine control of enabling it to treat only the fraction to which treating suited some specific conditions in the contents of the allowed modality.

[0087] Then, by embedding the field information and the local information which show the content of a contents by this data transfer limit technique at the header unit of stream data, and using these fields information and a local information In the stream which treating becomes from the contents of the allowed modality (only 1 time copy improper, copy-izing or a copy free-lancer) Processing of only the fraction which suits the conditions (a field, area) specified beforehand is enabled, and it is preventing from processing about other other fractions by the user etc.

[0088] The system configuration for realizing this data transfer limit technique is shown in drawing 11 . First, the transfer control according to the field information added to the bucket header unit of stream data is explained.

[0089] It says here.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The block diagram showing the system configuration of the computer system concerning the 1 operation gestalt of this invention.

[Drawing 2] Drawing showing the relation of the software and hardware in the system of drawing 1 .

[Drawing 3] Drawing showing an example of the device authentication used by the system of drawing 1 , and key exchange.

[Drawing 4] The flow chart which shows an example of the concrete procedure of authentication processing used by the system of this operation gestalt.

[Drawing 5] Drawing showing an example of the stream configuration of the digital contents applied to the system of this operation gestalt.

[Drawing 6] Drawing showing a mode that contents identification information was added to the packet HDR of the digital contents applied to the system of this operation gestalt.

[Drawing 7] Drawing for explaining the principle of digital contents limit processing applied to the system of this operation gestalt.

[Drawing 8] Drawing for explaining the contents record operation to the storage device prepared in the system of this operation gestalt.

[Drawing 9] Drawing for explaining the storage method of the key in the storage device prepared in the system of this operation gestalt.

[Drawing 10] Drawing for explaining a regeneration operation of the contents currently recorded on the storage device prepared in the system of this operation gestalt.

[Drawing 11] Drawing for explaining the principle of the data transfer limit technique applied to the system of this operation gestalt.

[Drawing 12] Drawing showing an example of the structure of the stream data used by the data transfer limit technique of drawing 11 .

[Drawing 13] Drawing showing the data limit processing operation by the data transfer limit technique of drawing 11 .

[Drawing 14] The flow chart which shows the procedure of the data transfer limit technique of drawing 11 .

[Drawing 15] The block diagram showing the system configuration of the computer system which prepared encryption/decryption function in 1394 bridges.

[Description of Notations]

11 -- Personal computer (PC)
12 -- Set top box (STB)
13 -- A digital camcorder or DV camcorder (DVC)
14 -- Digital video cassette recorder (D-VCR)
111 -- CPU module
112 -- Main memory
113 -- ********** or digital TV tuner
114 -- VGA controller
115 -- MPEG 2 decoder
116 -- DVD-RAM drive
117--1394 bridge
121 -- Authentication section (Authenticator)
122 -- Encryption / decryption section (De-/Cipher)
131 -- Authentication section (Authenticator)
132 -- Encryption section (Cipher)
141 -- Authentication section (Authenticator)
142 -- Encryption / decryption section (De-/Cipher)
1111 -- Authentication section (Authenticator)
1112 -- Decryption section (De-cipher)
1131 -- Authentication section (Authenticator)

1132 -- Encryption section (Cipher)
1151 -- Authentication section (Authenticator)
1152 -- Decryption section (De-cipher)
1161 -- Authentication section (Authenticator)

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CORRECTION or AMENDMENT

[Official report class] Printing of the amendment by the convention of 2 of Article 17 of a patent law
[Section partition] The 6th section 3rd partition
[Issue date] February 23, Heisei 13 (2001. 2.23)

[A open number] Publication number 11-306092
[A open day] November 5, Heisei 11 (1999. 11.5)
[**** format] Open patent official report 11-3061
[Application number] Japanese Patent Application No. 10-108116
[The 7th edition of International Patent Classification]

G06F	12/16	320
	12/14	320

[FI]

G06F	12/16	320 B
		320 E
	12/14	320 B
		320 E

[Procedure revision]
[Presentation day] March 24, Heisei 12 (2000. 3.24)
[Procedure amendment 1]
[The document name for an amendment] Specification
[The subject name for an amendment] Claim
[The amendment technique] Change
[Content of an amendment]
[Claim]
[Claim 1] In the data processor which has the interface which can connect the device which has an authentication function for enciphering, delivering and receiving the data for a copy protection Bus,
Two or more functional modules which are combined with this bus, respectively, and transmit or receive the data for a copy protection via [aforementioned] a bus,
It is prepared for every aforementioned functional module, and an authentication means to perform authentication processing for enciphering, delivering and receiving the data for [aforementioned] a copy protection between the functional modules of the partner point or the aforementioned devices which deliver and receive the data for [aforementioned] a copy protection is provided.
The data processor characterized by performing authentication processing for every functional

module in the aforementioned data processor.
[Claim 2] The data processor of the claim 1 publication characterized by for an encryption means encipher the data for [aforementioned] a copy protection to be prepared in the functional module of the transmitting side which transmits the data for [aforementioned] a copy protection through the aforementioned bus, and to be prepared the decryption means for decrypting the data by which encryption was carried out [aforementioned] and canceling the encryption in the functional module of the receiving side which minds the aforementioned bus, and receives and processes the data for [aforementioned] a copy protection.
[Claim 3] A bus interface means to connect the aforementioned device with the aforementioned bus transparent is provided further.
When delivering and receiving the data for a copy protection between the aforementioned device and each aforementioned functional module, encryption data are transmitted on the aforementioned bus.
The data processor of the claim 2 publication characterized by using the same authentication and an encryption protocol on the both sides between [aforementioned] functional modules and between the aforementioned device and the aforementioned functional module.
[Claim 4] The decoder which decodes CPU module and the coded data by which digital compression coding was carried out in the functional module treating the data for [aforementioned] a copy protection, and the data processor of the claim 1 publication characterized by containing at least one of storage devices.
[Claim 5] The data once which can be copied, and the data which cannot be copied are in the modality of data for [aforementioned] a copy protection, and the identification information for specifying the modality of data which can be treated by the functional module is assigned to each aforementioned functional module.
The aforementioned authentication means,
The data processor of the claim 1 publication characterized by performing key exchange for making the functional module of a receiving side generate an encryption cancel key required when it is the functional module which it distinguishes whether it is a functional module with the functional module of the receiving side able to treat the data for sending based on the identification information corresponding to the functional module of a receiving side, and can treat the data for sending, in order to decrypt encryption data between the functional modules of a receiving side.
[Claim 6] An encryption cancel key required in order to decrypt the enciphered data is changed for every modality of data for sending.
The data processor of the claim 1 publication characterized by generating the encryption cancel key of the number corresponding to the number of modalities of the data which can process the functional module of a receiving side by the aforementioned authentication processing in the modality of data which constitute the aforementioned stream on the functional module of the aforementioned receiving side when transmitting the stream which consists of two or more sorts of data with which a modality is different.
[Claim 7] The data class information which shows the modality of data is embedded at the aforementioned stream.
The functional module of the aforementioned receiving side is the data processor of the claim 6 publication characterized by changing the encryption cancel key to use dynamically based on the aforementioned data class information.
[Claim 8] The aforementioned data processors are CPU module, the decoder which decodes the coded data by which digital compression coding was carried out, and a personal computer which has a storage device as the aforementioned functional module.
This personal computer is the data processor of the claim 1 publication characterized by having a PCI bus and having an IEEE1394 serial bus as an interface with the aforementioned device as the aforementioned bus.
[Claim 9] In the data processor which has a bus and two or more functional modules combined with this bus, respectively

Each functional module which treats digital contest ****** for a copy protection in two or more aforementioned functional modules possesses an authentication means to perform authentication processing for enciphering, delivering and receiving the aforementioned digital contest ****** between the functional modules of the partner point which delivers and receives digital contest ****** through the aforementioned bus.
The contents once which can be copied, and the contents which cannot be copied are in the modality of digital contents for [aforementioned] a copy protection, and the modality of contents which can be treated by the functional module is specified for every aforementioned functional module.
The aforementioned authentication means,
The data processor characterized by distinguishing whether it is a functional module with the functional module able to treat the contents for sending for every functional module of a receiving side.
[Claim 10] In the copy protection technique applied to the data processor possessing a bus, two or more functional modules which are combined with this bus, respectively, and transmit or receive the data for a copy protection via [aforementioned] a bus, and a bus interface means by which the device which has the data encryption / decryption function for a copy protection is connectable
When delivering and receiving the data for a copy protection between [aforementioned / two or more] functional modules or between the aforementioned functional module and the aforementioned device, authentication processing for checking the justification of a mutual functional module between [for a communication] devices is performed.
When the justification of a mutual device is checked by this authentication processing, transmit data is enciphered in the device of a transmitting side, and it transmits to the device of the partner point.
The encryption data is decrypted in the device of a receiving side.
The copy protection technique characterized by carrying out the copy protection of the data which flow on the aforementioned bus.
[Claim 11] It is the copy protection technique of the digital contents applied to the system which consists of a bus and two or more devices connected to this bus.
When the stream which consists of two or more sorts of digital contentss from which a modality is different is enciphered and it transmits to the device of a receiving side, the device of a transmitting side Only the number of modalities of the contents which precedes the sending and it can treat for every device of a receiving side by performing authentication processing The encryption cancel key corresponding to the number of modalities of the data which can process the device of a receiving side in the modality of digital contents which constitutes the aforementioned stream is notified to the device of each receiving side.
The device of a receiving side is the copy protection technique characterized by changing the encryption cancel key to use according to the modality of digital contents which received.
[Claim 12] The class information which shows the modality of digital contents is embedded at the aforementioned stream.
The device of a receiving side is the copy protection technique of the claim 11 publication characterized by changing dynamically the encryption cancel key used for decryption processing based on the aforementioned data class information.
[Claim 13] In the data processor which transmits data to a receiving set side so that the unjust copy of the digital contents passed on a bus may be prevented
A key transmitting means to transmit the encryption cancel key corresponding to the modality of digital contents to judge and by which processing is permitted to the aforementioned receiving set from which the data for a copy protection with which it attests whether processing of the data for a copy protection is permitted between the aforementioned receiving sets, and processing is permitted to the aforementioned receiving set distinguish what kind of digital contents it is to the aforementioned receiving set, respectively,
The data processor to which the aforementioned receiving set is characterized by providing a transmitting means to transmit the digital contents which can cancel an encryption using the

aforementioned encryption cancel key.
[Claim 14] As the unjust copy of the digital contents passed on the internal bus of a computer system is prevented, it is the copy protection technique of transmitting data to a receiving set side proper.
It attests whether processing of the data for a copy protection is permitted between the aforementioned receiving sets, and the data for a copy protection with which processing is permitted to the aforementioned receiving set distinguish what kind of digital contents it is.
The aforementioned receiving set transmits only the encryption cancel key corresponding to the modality of digital contents to which processing is permitted to the aforementioned receiving set, respectively.
The copy protection technique that the aforementioned receiving set is characterized by transmitting the digital contents which can cancel an encryption using this encryption cancel key.
[Claim 15] In the data processor which carries out reception of the data transmitted from the sending set side so that the illegal copy of the digital contents passed on a bus might be prevented
A means to transmit the information which shows the modality of digital contents for [to attest / by which processing is permitted to this data processor] a copy protection which attests whether processing of the data for a copy protection is permitted between the aforementioned sending sets to the aforementioned sending set,
The data processor characterized by providing a decryption means to receive the encryption cancel key corresponding to the modality of digital contents for [by which processing is permitted to the aforementioned data processor based on this transmit information] a copy protection, and the digital contents of which the aforementioned data processor can cancel an encryption using this encryption cancel key from the aforementioned sending set, and to decrypt the aforementioned digital contents, respectively.
[Claim 16] As the unjust copy of the digital contents passed on the internal bus of a computer system is prevented, it is the copy protection technique which carries out reception of the data proper from a sending set side.
It attests whether processing of the data for a copy protection is permitted between the aforementioned sending sets, and the information which shows the modality of digital contents for [to which the reception of data is permitted] a copy protection is transmitted to the aforementioned sending set.
Based on this transmit information, the encryption cancel key corresponding to the modality of digital contents to which the aforementioned reception is permitted is received from the aforementioned sending set, respectively.
The digital contents of which a receiving set can cancel an encryption using this encryption cancel key is received from the aforementioned sending set.
The copy protection technique characterized by decrypting the aforementioned digital contents using the aforementioned encryption cancel key.
[Procedure amendment 2]
[The document name for an amendment] Specification
[The subject name for an amendment] 0020
[The amendment technique] Change
[Content of an amendment]
[0020]
[The means for solving a technical problem] In the data processor which has the interface which can connect the device which has an authentication function for this invention enciphering, delivering and receiving the data for a copy protection in order to solve an above-mentioned technical probrem A bus and two or more functional modules which are combined with this bus, respectively, and transmit or receive the data for a copy protection via [aforementioned] a bus, Between the functional modules of the partner point or the aforementioned devices which are prepared for every aforementioned functional module, and deliver and receive the data for [aforementioned] a copy protection An authentication means to perform authentication processing for enciphering, delivering and receiving the data for [aforementioned] a copy

protection is provided, and it is characterized by performing authentication processing for every functional module in the aforementioned data processor.
[Procedure amendment 3]
[The document name for an amendment] Specification
[The subject name for an amendment] 0021
[The amendment technique] Change
[Content of an amendment]
[0021] In this data processor, the authentication means is prepared in the interface section of two or more functional modules of each treating the data for [, such as a digital contents,] a copy protection, and authentication processing is individually performed between functional modules or between a functional module and the aforementioned device. Therefore, on the bus to which these functional modules were connected, the key and digital contents for encryption cancel come to be transmitted while it had been enciphered by them, and they can prevent the illegal copy of a digital contents. Moreover, since authentication processing is performed for every functional module, it is enabled to restrict efficiently the modality (only 1 time a copy good, copy improper, a copy free-lancer) of digital contents which can be treated by it per functional module.
[Procedure amendment 4]
[The document name for an amendment] Specification
[The subject name for an amendment] 0022
[The amendment technique] Change
[Content of an amendment]
[0022] Moreover, it is enabled to enable it to use the same authentication and an encryption protocol on the both sides between [aforementioned] functional modules and between the aforementioned device and the aforementioned functional module by providing further a bus interface means to connect an account device with the aforementioned bus transparent. That is, it is enabled to treat similarly, without distinguishing the functional module and the aforementioned device in a data processor, if it sees from each functional module or application program in a data processor.
[Procedure amendment 5]
[The document name for an amendment] Specification
[The subject name for an amendment] 0026
[The amendment technique] Change
[Content of an amendment]
[0026] Moreover, this invention is set to the data processor which transmits data to a receiving set side so that the unjust copy of the digital contents passed on a bus may be prevented. It attests whether processing of the data for a copy protection is permitted between the aforementioned receiving sets. The data for a copy protection with which processing is permitted to the aforementioned receiving set A key transmitting means to transmit the encryption cancel key corresponding to the modality of digital contents to judge and by which processing is permitted to the aforementioned receiving set which distinguishes what kind of digital contents it is to the aforementioned receiving set, respectively, The aforementioned receiving set is characterized by providing a transmitting means to transmit the digital contents which can cancel an encryption using the aforementioned encryption cancel key.
[Procedure amendment 6]
[The document name for an amendment] Specification
[The subject name for an amendment] 0028
[The amendment technique] Change
[Content of an amendment]
[0028] Moreover, this invention is set to the data processor which carries out reception of the data transmitted from the sending set side so that the illegal copy of the digital contents passed on a bus might be prevented. The private seal proof which attests whether processing of the data for a copy protection is permitted between the aforementioned sending sets, A means to transmit the information which shows the modality of digital contents for [by which processing is permitted to

this data processor] a copy protection to the aforementioned sending set, The encryption cancel key respectively corresponding to the modality of digital contents for [by which processing is permitted to the aforementioned data processor based on this transmit information] a copy protection, The digital contents of which the aforementioned data processor can cancel an encryption using this encryption cancel key is received from the aforementioned sending set, and it is characterized by providing a decryption means to decrypt the aforementioned digital contents.

[Translation done.]